EUROPEAN PARLIAMENT

Briefing
October 2014

Cyber defence in the EU
Preparing for cyber warfare?

SUMMARY

In recent years, cyber attacks on a serious scale have become a matter of concern to states, due to the threat they can pose to national security, but also a potential foreign policy and military tool to be added to existing options in their arsenals. While international law is still struggling with defining norms on state actions in cyberspace, the latter is now increasingly viewed as a fifth domain of warfare.

Although, for the time being, no cyber attack is known to have provoked death or physical damage to human beings, an ever growing number of states around the world are preparing for conflict in the cyber domain, and, in this context, have been developing national doctrines, cyber-defence strategies and defensive and offensive capabilities for cyber warfare.

The definitions surrounding 'cyber war' and 'cyber defence' are still widely debated, and indeed have become a burgeoning topic for international legal scholars, along with governments and international organisations. With little agreement among the major countries preparing their own cyber warfare capabilities, there are not yet rules comparable to those for conventional warfare. A number of EU Member States are amongst those developing their capabilities, while the EU's own Defence Agency is also working on projects to augment cyber-defences in the Union. NATO too is involved in efforts to develop defensive capabilities.

In this briefing:

- Issue
- Cyber warfare: an unclear concept
- Developing cyber capabilities around the world
- Cyber defence in the EU: national policies and the common approach
- NATO's cyber defence policy
- Main references

EPRS | European Parliamentary Research Service
Author: Carmen-Cristina Cîrlig
Members' Research Service

Issue

In today's highly interconnected world, cyberspace and the wide array of risks and threats associated with it have become more and more preoccupying for states. The increasing range and sophistication of threats in the cyber realm – from malware to distributed denial of service (DDoS) attacks to advanced persistent threats (APT)[1] – have prompted efforts to protect against the risks posed to businesses and governments alike: economic and military espionage, theft of intellectual property, interference with critical infrastructure, and destruction of data. In this context, states are developing cyber-defence and cyber-offence capabilities to prepare for the advent of 'cyber war'.

Cyber warfare: an unclear concept

Growing cyber threat

Cyber security, to counter cyber attacks perpetrated by various actors (e.g. criminals, 'hacktivists' or governments), has become an important policy issue in many states. Besides the vast economic costs of cyber crime and cyber espionage (estimated at between US$300 billion and US$1 trillion), 57% of industry experts believed in 2012 that 'an arms race was taking place within cyberspace'.

Emerging from the purely technical, concerns over ensuring the security of government systems, of critical infrastructure and critical industries, and of private citizens, are now the subject of political, diplomatic, economic and military debate, at national and international levels. Terms such as cyber security, cyber attack, cyber crime, cyber war (or warfare) and cyber terrorism have entered the public discourse; however, there is no consensus on their definitions, making it difficult to create a conceptual framework in which relations and international agreements related to cyberspace can be developed. Military forces around the world are also concerned about increasing vulnerabilities related to cyberspace and the internet. In this context, claims that cyberspace is the fifth domain of warfare next to land, sea, air and space operations have led to a growing debate about the advent of cyber warfare.

Cyberspace: the fifth domain of war?

Cyber attacks have become both a concern for national security and a new tool in foreign policy. Major cyber-incidents in the past few years have led to this assumption. In 2007, DDoS attacks against the Estonian government led to paralysis of public services in Estonia for three weeks, and marked the start of collaborative efforts to address the cyber warfare threat and to develop international norms for conduct in cyberspace. During the 2008 Russian–Georgian war, media and government websites in Georgia came under attack from hackers. In 2010, the 'Stuxnet' computer worm, considered one of the most sophisticated cyber weapons to date and a possible first sight of cyber warfare, damaged uranium enrichment centrifuges at Iran's Natanz nuclear site. (Stuxnet has been compared to a 'cyber missile', aimed at destroying the physical infrastructure of Iran's nuclear plants). And in 2012, a DDoS campaign against the US financial sector (Operation Ababil) was claimed by the group 'Izz ad-Din Al Qassam', but it is suspected that Iran was behind it, in retaliation for the Stuxnet attack.

Although these incidents have not been attributed to particular states, suspicions persist that state actors sponsored them (besides Iran, Russia for the Estonian and Georgian cases, and the US and Israel with regard to the Stuxnet attack). Recently, cyber attacks are said to have been used in the conflict in Ukraine, both by Russia and Ukraine, and also against NATO, whose websites were targeted by DDoS attacks in

March 2014. In other conflicts in the Middle East, evidence points to cyber attacks being deployed in Israel, Syria and Iraq, again not clearly attributed to state sponsored actors (although, for example, involvement of Iranian and Turkish 'cyber forces' is alleged in the case of DDoS attacks against Israel). The EU and some of its Member States have also been targets of cyber-attacks. Besides some economically driven cyber attacks (e.g. on the EU's carbon Emission Trading Scheme), others have been directed to the military: grounding French naval planes, securing access to the UK Ministry of Defence's classified networks or attacking the Estonian Ministry of Defence (2013).

Research conducted on the most conflict-prone pairs of states between 2001 and 2011 has concluded that, on the one hand, the number of cyber attacks directed against each other was not that high (the most frequent cyber attacks were launched between China and the US, followed by North Korea targeting South Korea) and, on the other hand, the effects of the attacks have not lead to death or serious damage to physical property, although they have temporarily disrupted the target network's systems. Another argument goes further in asserting that despite their immediate success, such cyber-attacks did not lead to the intended (longer-term) foreign policy outcome.

Against this background, experts are divided over the reality of 'cyber war'. While recognising the risks connected to the new cyber threats and the necessity of cyber security, 'cyber war' is, in some experts' view, an 'inappropriate analogy'. For others, although cyber war will not replace conventional 'kinetic' (traditional war) operations, armies will increasingly make use of cyber operations to support deployments. Currently there is a 'black hole' over what constitutes an act of cyber war and what the appropriate response might be, a definition of what constitutes cyber warfare and whether it encompasses more than states as actors. For example, the US Department of Defense has defined cyber warfare as: 'an armed conflict conducted in whole or in part by cyber means. Military operations conducted to deny an opposing force the effective use of cyberspace systems and weapons in a conflict. It includes cyber attack, cyber defence and cyber enabling actions.' The US goes on to define **defensive** and **offensive capabilities**, as well as the need for pre-emptive action in certain cases.

In US terminology, **defensive counter-cyber** (DCC) are 'all defensive countermeasures designed to detect, identify, intercept, and destroy or negate harmful activities attempting to penetrate or attack through cyberspace'. **Offensive counter-cyber** (OCC) are 'offensive operations to destroy, disrupt or neutralise adversary cyberspace capabilities both before and after their use against friendly forces, but as close to their source as possible.' **Offensive cyberspace operations** represent 'activities that, through cyberspace, actively gather information from computers, information systems or networks, or manipulate, disrupt, degrade or destroy targeted computers, information systems or networks. This includes cyber operational preparation of the environment, offensive counter-cyber, cyber attack and related electronic attack and space control negation'.

States such as Russia and China have different understandings of cyberspace to the US, and seem to refer to cyber warfare primarily as the way the Western World refers to conflict in the cyber domain. Russia does not have a definition of cyber warfare, while China makes references to 'network warfare operations' and 'cyber warfare attacks'. An initiative to bridge the conceptual divide on cyber warfare between the US and Russia did not succeed, as the definitions developed by Russian and American experts differed substantially.[2] Despite lack of agreement on concepts, many states increasingly consider cyber defence as an important capability, and are allocating significant budget and personnel to developing not only cyber defence, but also cyber-offence capabilities.

International Law and cyber warfare

International Law is struggling to address the issue of 'cyber war', both as concerns *jus ad bellum* (the rules governing international armed conflict) and *jus in bello* (the way in which war is waged, namely international humanitarian law). Among the questions that need clarification is whether existing international law also applies to cyber operations and, if yes, in what conditions.

The Tallinn Manual process, an effort to define norms governing cyber warfare, has posited that the general principles of international law do apply to cyberspace, including *jus ad bellum* and *jus in bello*. The manual's 95 rules define state responsibility in cyber operations contrary to International Law, applying the principle of prohibition of the use of force, the circumstances in which self-defence may be invoked, the conduct of parties during cyber hostilities, etc. It asserts, *inter alia*, that 'an international armed conflict exists whenever there are hostilities, which may include or be limited to cyber operations occurring between two states or more', and that 'cyber operations alone might have the potential to cross the threshold of international armed conflict', although such conflict triggered solely in cyberspace has not yet occurred. Under the manual, a cyber operation can be retaliated in self-defence, but only if the conditions of a cyber armed attack ('use of force' resulting in serious physical injury and damage) are met.

These rules remain open to interpretation, to the evolution of technology and cyber capabilities, as well as to criticism. Some scholars contest the lack of distinction between cyber and kinetic attack, and thus the possibility to respond to a cyber attack through a traditional military operation. For them, a middle way should be found between the Tallinn rules and the opposite assumption that 'what happens in cyber-space stays in cyberspace'. Other experts have focused on the challenge of **attribution** (i.e. attributing to states the responsibility for a cyber attack, organised by a non-state group); the possibility of invoking self-defence; and the circumstances in which a state responsible for the actions of a proxy group triggers a 'war' with the attacked state.

Developing cyber capabilities around the world

Cyber defence has been defined as 'the application of security measures to protect against, and react to cyber attacks against communications and command systems infrastructure.' Many countries have included cyber defence in their defence planning and budgets, including the development of offensive cyber capabilities. A UNIDIR 2012 assessment surveyed publicly available information for the 193 members of the United Nations and found that 114 states had national cyber-security programmes. Forty-seven of these give a role to the armed forces, while 67 states have solely civilian programmes. The same study suggests that 12 of the 15 largest military spenders have, or are developing, dedicated cyber-warfare units and that, of these, 10 appear to possess or be developing offensive cyber capabilities. The US, UK, China, Russia and France are often seen as most advanced in terms of cyber power and cyber capabilities.

United States

The US has militarised the response to cyber-attacks through its Cyber Command (USCYBERCOM), launched in 2010 and bringing together the cyber components of the US Navy, the US Marine Corps, the army and air force into a unified command. USCYBERCOM is one of the largest cyber-defence organisations in the world.

In 2011, the US Department of Defense (DoD) adopted the 'Strategy for operating in Cyberspace' which rests upon five strategic initiatives: cyberspace will be treated in a similar manner to air, land, maritime and space domains; the DoD will employ new defensive methods for dealing with cyber threats; cooperation at national and international levels will be encouraged; finally, the DoD will focus on developing a pool of skilled personnel and technological innovations. Although predominantly defensive (the Pentagon is said to possess 90% offensive and 10% defensive cyber capabilities), the creation of a strong offensive deterrent has been advocated by high-ranking military officials in the US. The DoD's new cyber strategy does not explain how offensive capabilities might be used or the 'active' cyber defence posture. The Snowden leaks offer information about the US MonsterMind programme, designed for automated response to cyber attacks against the US. The Pentagon has also increased spending on cyber operations ($26 billion over the next five years) and pledged to build a 6 000-strong cyber force by 2016. Besides the development of offensive and defensive cyber capabilities, the US pursues a norm-setting agenda internationally, to set rules about what kind of cyber operations constitute an act of war. Moreover, a 2013 presidential directive instructs the US to aid allies who come under foreign cyber attack.

China

China has invested large sums in personnel and information infrastructure for cyber warfare. In addition to People's Liberation Army (PLA) operators, in particular the PLA's Unit 61398, there is a large network of volunteer Militia Information Technology Battalions, or 'net militia units', recruited from civilian talent pools. China is viewed by Pentagon officials as the main cyber threat to the US. On the other hand, in 2007, China denounced the US as an important source of cyber attacks against it. Recently, the Snowden revelations of US cyber espionage against China have complicated the US-China cyber dialogue. Nevertheless, the first meeting of the US-China Cyber Working Group still took place in July 2013, although China suspended its participation in the group in 2014, following US indictments against five Chinese hackers accused of economic espionage and cyber-theft of trade secrets. Besides the US, Chinese cyber attacks have targeted countries all over the world. Analysts suggest that Chinese attacks are less sophisticated technologically, but highly effective due to their large volume.

Russia

Cyberspace has become in Russia's interpretation a 'new theatre of war' and one of the priorities for military R&D. The Military Doctrine of 2010 discusses the use of political and informational instruments to protect national interests and those of allies. The doctrine defines the characteristic features of modern military conflict as including the integrated use of military force and non-military capabilities, and a greater role for information warfare. Creation of a cyber-security command and a new cyber branch within the armed forces will enhance the preparedness of Russian armed forces to defend against attacks from cyberspace (and outer space). Moreover, in efforts to secure its networks, Russia has been buying typewriters. Conversely, Russia is thought to use complex and advanced cyber attacks in support of its national interest and military goals; for example there is evidence that Russian military operations in Georgia during the 2008 war were supported by cyber operations. In 2013, the US and Russia agreed to create a cyber 'hotline' to help defuse any cyber-related crises in the future.

Middle East: Israel, Iran, Syria and Turkey

Israel is a constant target of cyber attacks, reportedly fighting 1 000 attacks every minute. In September 2014, the government created a National Authority for Cyber Defence, aimed at protecting civilians against cyber attacks, while an elite cyber-defence unit has been set up within the Israeli Secret Service. Israel has also reportedly used cyber attacks for political and military purposes, including being implicated in the Stuxnet attack, and is among the most technologically advanced countries in the field.

Iran has been a target of the most advanced malware (e.g. Stuxnet, Duqu, Flame) and it has reportedly chosen to respond in kind, with cyber attacks perpetrated by non-state groups such as 'Izz ad-Din al-Qassam' and the 'Iranian Cyber Army'. The latter group is believed to be linked to the Iranian military. In March 2012, a decree was issued establishing the Supreme Council of Cyberspace, tasked with the coordination of national cyber warfare and information security. Iran announced in June 2011 that it planned to establish a cyber command for the armed forces to defend against cyber attack and to centralise operations. Iranian cyber capabilities are coordinated within the military by the Passive Defence Organisation. **Syria's** most prominent hacker group is the Syrian Electronic Army (SEA), loyal to Assad and responsible for cyber attacks on governments and media critical of his regime. There is also possible SEA involvement in cyber attacks against Islamic State, to collect intelligence on behalf of the Syrian and Iranian governments. **Turkey's** military strategy, revised in October 2010, added cyber-security threats. Turkey established a cyber defence unit in 2012 within the armed forces.

The Korean Peninsula

South Korea is one of the most networked countries in the world and has been the target of cyber attacks allegedly stemming from North Korea. The government has attributed the attacks to Pyongyang's Reconnaissance General Bureau, a branch of the military. In South Korea, the National Cyber Security Centre (NCSC) coordinates the civilian response to cyber incidents. The Ministry of Defence established the Cyber War Centre in 2010, with the aim of increasing the security of government and financial information networks, and an independent Cyber Warfare Command with over 200 personnel, for defensive and offensive operations in cyberspace. In February 2014, reports claimed the South Korean military was committed to developing 'sophisticated cyber-warfare tools'.

North Korea appears to have been using cyber-attacks as a new weapon to disrupt network systems, in particular in South Korea and the US, as well as to gain access to sensitive information. Reports point to a cyber warfare department of 3 000 personnel. The North Korean regime sees cyber-attacks as an effective tool, and has apparently disconnected its own critical servers from the internet.

Cyber defence in the EU: national policies and the common approach

Member States' national policies on cyber defence/warfare

There are various national practices on cyber defence among the EU Member States (MS). Almost all MS have adopted a national cyber security strategy, or mention cyber-security as an important aspect of their national security strategies, or have put in place structures to deal with cyber threats. Around 15 MS have included a military perspective of cyber defence in their national approaches, but only a few admit to investing in cyber weapons or define cyberspace as a potential warfare domain.

- **Denmark's** Defence Agreement for 2013-2017 establishes a Centre for Cyber Security under the Ministry of Defence (MoD), as well as strengthens military capabilities through a Computer Network Operations capability to provide the capacity to execute **defensive and offensive military operations in cyberspace**;
- **Estonia's** 2008 Cyber Security Strategy is currently being renewed. The Estonian MoD and the Defence Forces are responsible for 'coordinating cyber defence in the area of

national defence', with the voluntary Defence League's Cyber Unit being tasked *inter alia* with the development of cyber capabilities;

- **Finland** announced in 2011 that it will invest in the development of cyber-defence weapons. Its 2013 national cyber security strategy states that the Finnish Defence Forces 'will create a **comprehensive cyber-defence capability**', which will comprise cyber intelligence, cyber warfare and protection capabilities. A cyber defence unit to specialise in cyber warfare will be operational in 2015.
- **France's** 'Information systems defence and security' strategy (2011) contains four objectives for France in cyberspace: to become a global power in cyber defence; safeguard France's ability to make decisions through the protection of information related to its sovereignty; strengthen the cyber security of critical national infrastructure and ensure security in cyberspace. Moreover, France's White Paper on Defence (2013) characterises cyber attacks as the third most important threat to national security. France will develop cyber-intelligence capabilities, as well as **'offensive capabilities'**. The main authority for cyber defence is the French Network and Information Security Agency (ANSSI, set up in 2009), responsible for detecting and responding to cyber attacks, supporting R&D and providing information to other governmental bodies. Other units and agencies within the armed forces focus either on cyber warfare or on cyber defence of the state's military networks. In January 2014, the Defence Ministry earmarked more than €1 billion for cyber defence;
- **Germany's** 2011 cyber security strategy establishes a National Cyber Security Council and a National Cyber Response Centre to coordinate cyber policy and, respectively, to ensure operational cooperation in areas of vulnerability protection and incident response. The German military's Strategic Reconnaissance Unit is apparently a specialised cyber group trained in offensive cyber capabilities;
- **Greece's** military started to invest in cyber warfare capabilities in 1999, with the creation of the Office of Computer Warfare. Today, the Directorate of Cyber Defence is under direct supervision of the Chief of Defence;
- **Italy** has set up a military electronic warfare unit responsible for intelligence, surveillance, target acquisition and reconnaissance. Its 2013 National Strategic Framework for Cyberspace Security, the National Plan for cyber protection and information security and the defence directives on cyberspace form the policy framework on cyber security and cyber defence. They point to the necessity to develop cyber-intelligence and cyber-defence capabilities, and the command and control structures 'to plan and conduct military operations in cyberspace'.
- **Lithuania** adopted in 2011 a Programme for the Development of Electronic Information Security for 2011–2019. In 2015, Lithuania will establish a National Cyber Security Centre to prepare for cyber operations and defend against cyber attacks;
- The **Netherlands** adopted a Defence Cyber Strategy in 2012 establishing six priorities: adopting a comprehensive approach; strengthening cyber-defence capabilities; developing cyber-**offensive military capabilities**; strengthening intelligence capabilities in cyberspace; encouraging innovation and recruitment of qualified personnel; and intensifying cooperation at national and international level. A joint Defence Cyber Command, launched in September 2014, within the Dutch Army, is responsible for the development of cyber capabilities;

- The **UK's** 2011 Cyber Security Strategy characterises cyber attacks as a national security threat, and aims at, *inter alia*, defending national infrastructure from cyber attacks and improving capabilities to 'deter and disrupt attacks on the UK'. A Global Operations and Security Control Centre and a Defence Cyber Operations Group of the MoD respectively defend the Ministry's network, and integrate the MoD's 'cyber activities across the spectrum of defence operations.' The UK announced in 2013 its intention to incorporate **cyber warfare as part of future military operations** and to develop a 'cyber strike force' to respond to potential military use of cyber capabilities. According to the Military Balance 2014, the UK government announced, in 2011, a £650 million investment in a national cyber-security programme (and possibly an additional £150 million in cyber-security measures) over four years. In 2014, the UK announced £2 million in funding for R&D focused on automated cyber defence response systems;
- Other Member States (**Austria**, **Croatia**, **Hungary**, **Poland**, **Slovakia**, **Spain**) have also integrated a defence component in their cyber strategies.

A future EU Cyber Defence Policy Framework

The European Union has recognised cyber attacks are a key threat to its security interests and realised the importance of a comprehensive EU approach to cyber security. However, the EU has taken action predominantly to fight cybercrime and protect critical information infrastructure, by defining the legal and operational framework guiding cooperation between MS and with competent EU bodies (e.g. European Network and Information Security Agency, the European Cybercrime Centre). While cyber security constitutes a priority in its internal security strategy, EU action within the Common Foreign and Security Policy (CFSP) has been limited, due to the reluctance of Member States to cooperate in this field.

Nevertheless, the comprehensive EU Cyber Security Strategy (2013) contains a number of strategic priorities, including cyber defence in the framework of the Common Security and Defence Policy (CSDP). Efforts should focus accordingly on building cyber defence capabilities in the MS; building the EU cyber defence policy framework; promoting civil-military dialogue, as well as dialogue with international partners, including NATO, and other stakeholders. In 2011, cyber defence was included among the priority projects for the European Defence Agency (EDA) in capabilities development.[3] In 2012, MS also agreed on the **EU Concept for Cyber defence in EU-led military operations**, so that operational commanders create and maintain situational cyber awareness. In 2013, an EDA stock-taking study on cyber capacities across Member States and EU institutions found that military cyber defence at European level was still in its infancy and recommended a series of actions be taken at EU level (enhancing EU network protection, strengthening intelligence and incident response capabilities, creating a culture of cyber-security, and reinforcing links between NATO and the EU) and by MS (development of cyber-defence training and education initiatives; information exchange, as well as sharing facilities). EDA is focusing currently on specific projects (within the Pooling and Sharing concept) related to: training and exercises, improving situational awareness for CSDP operations, a Cyber Defence Research Agenda, developing solutions against APT malware and work on cryptography and protection of information.

In December 2013, the European Council called for an **EU Cyber Defence Policy Framework** to be set up in 2014, including a roadmap and concrete projects focused on training and exercises, improving civil/military cooperation on the basis of the EU Cyber-security Strategy, as well as the protection of assets belonging to EU missions and operations. According to experts, the Cyber Defence Policy Framework will focus on: the development of MS' cyber-defence capabilities, research and technologies; reinforced protection of communication networks supporting CSDP structures, missions and operations; mainstreaming of cyber security into EU crisis management; raising awareness through improved training, education and exercises for MS; synergies with wider EU cyber policies and relevant actors and agencies in Europe; cooperation with relevant international partners, notably NATO. The same experts note that a major challenge in this context will be to find and retain high-quality cyber specialists for the armed forces. Finally, the basic premise of cooperation in cyber defence is that MS trust each other and are aware of their shared interests in cooperating in this matter.

The **European Parliament** has recently adopted with amendments (2014) the Directive on a high common level of network information security across the Union proposed by the Commission in 2013, yet to be agreed by Council. In Resolutions on Cyber security and defence (2012), EU military structures (2013), EU Cyber-security strategy (2013) and on the Implementation of the Common Security and Defence (2013), the EP has emphasised the importance of tackling the growing cyber-security threat, called for a common definition of cyber security and defence, as well as a common operating vision. It also stated that cyber defence should become an active capability of CSDP and reiterated the need to bridge the gap between internal and external aspects of cyber security.

NATO's cyber defence policy

NATO put cyber defence on its agenda following the 1999 cyber attacks against NATO during the Kosovo war. In 2002, NATO adopted a cyber defence programme, and created a NATO Computer Incident Response Capability (NCIRC), to prevent, detect and respond to cyber incidents. In 2008, NATO leaders approved the 'NATO Cyber Defence Policy', while, at the Lisbon Summit (2010), they decided to integrate cyber defence into NATO's defence planning process. In 2011, NATO approved its revised Cyber Defence Policy and Action Plan. NATO's main mission remains securing its own networks, although it aims also to assist Allies in ensuring a minimum level of cyber defence and in reducing vulnerabilities in their critical infrastructure.

NATO's 'enhanced cyber defence policy'

At the NATO Summit in Wales, in September 2014, the Allies endorsed an 'enhanced cyber defence policy', to improve NATO's governance of cyber defence, create partnerships with industry, help individual Allies to reinforce their cyber capabilities and focus more on training and education. In particular, NATO leaders endorsed the possibility of invoking Article 5 following a cyber attack, thus equating it with an 'armed attack' in certain situations. Nevertheless, ambiguity persists about the exact conditions that would trigger an Article 5 response and the nature of that response (military or cyber). Moreover, it seems the new cyber mandate would not allow NATO to mount an offensive attack on behalf of an Ally that has invoked Article 5, although NATO officials stated that individual Allies could decide to intervene. The new policy will also: include cyber defence in NATO's two-year defence planning cycle; increase bilateral cooperation, particularly via Smart Defence projects and information; introduce cyber defence into NATO's contingency planning; formalise NATO-industry cooperation; and implement a 'comprehensive cyber-defence training programme'.

Although NATO's political direction to develop its defence capacity is clear, it remains focused on NATO's own networks, as there is no agreement yet between member states to establish a viable cyber defence capability for NATO to deploy to help an Ally.

In this context, three options have been considered: NCIRC using its own assets and expertise to help an Ally in crisis; deploying multinational capabilities; and direct NATO access to national capabilities. For the moment, NATO encourages Allies to improve their own cyber defence capabilities and to coordinate their related national activities.

Multinational projects under NATO umbrella

The MN CD2 programme, founded in 2013 by Canada, Denmark, the Netherlands, Norway and Romania, has been identified as the 'key vehicle to advance cyber defence capabilities in multinational format.' The programme, developed in the framework of NATO's Smart Defence Initiative and open to all NATO members, aims at developing improved means of sharing technical information; shared awareness of threats and attacks; and advanced cyber-defence sensors. Other initiatives include the Malware Information Sharing Platform Smart Defence Initiative, with lead nation, Belgium; and the Cyber Defence Education and Training (CD E&T) Initiative, with lead nation, Portugal.

Cooperation and information-sharing have been recognised as important aspects of securing cyberspace. The 2008 NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) is open to NATO members and partners, but is officially an independent military organisation. As of June 2014, 14 nations have joined the Centre, which is a research and training facility, with activities ranging from legal and policy research on various cyber-related issues to support for NATO cyber exercises (e.g. Locked Shields). In June 2014, the creation of a new NATO military cyber warfare training centre in Estonia was approved. Both NATO and EU emphasise the importance of cooperation on cyber defence, which has been focused on joint exercises, exchange of best practices and mapping the extent of cyber attacks.

Main references

Cyber Security Review, Edition Summer 2014.

Tallinn Manual on the International law applicable to cyber warfare, 2013.

The Cyber Index: International Security Trends and Realities, UNIDIR, 2013.

The Military Balance 2014, International Institute for Strategic Studies (IISS), 2014.

Endnotes

[1] Malware means a software program whose goal is to infiltrate a computer or a network in order to collect or steal information or to take control of the system (e.g. worm, virus, Trojan horse); a Distributed Denial of Service (DDoS) attack is constituted by a stream of requests sent to a specific web server, leading to its serious slowdown or blockage; an Advanced Persistent Threat (APT) is a network attack whereby an unauthorised person gains access to a network and stays undetected for a long period of time, intending to achieve on-going access to the network.

[2] The US experts' definition of cyber warfare reads as 'cyber-attacks that are authorised by state actors against cyber infrastructure in conjunction with a government campaign', while the Russian experts stated that 'combat actions in cyberspace are cyber attacks carried out by states, groups of states, or organised political groups, against cyber infrastructure, which are part of a military campaign.'

[3] All EU Member States, with the exception of Denmark, participate in the European Defence Agency (EDA).

Disclaimer and Copyright

The content of this document is the sole responsibility of the author and any opinions expressed therein do not necessarily represent the official position of the European Parliament. It is addressed to the Members and staff of the EP for their parliamentary work. Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy. Photo credits: © XtravaganT/ Fotolia.

eprs@ep.europa.eu
http://www.eprs.ep.parl.union.eu (intranet)
http://www.europarl.europa.eu/thinktank (internet)
http://epthinktank.eu (blog)